Abstract

SYSTEM, METHOD AND PROGRAM PRODUCT FOR DETECTING MALICIOUS SOFTWARE

System, method and program product for detecting malicious software within or attacking a computer system. In response to a system call, a hook routine is executed at a location of the system call to (a) determine a data flow or process requested by the call, (b) determine another data flow or process for data related to that of the call, (c) automatically generate a consolidated information flow diagram showing the data flow or process of the call and the other data flow or process. After steps (a-c), a routine is called to perform the data flow or process requested by the call. A user monitors the information flow diagram and compares the data flow or process of steps (a) and (b) with a data flow or process expected by said user. If there are differences, the user may investigate the matter or shut down the computer to prevent damage.